PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-013486
(43)Date of publication of application : 17.01.1995

(51)Int.Cl. G09C 1/00
G06F 12/00

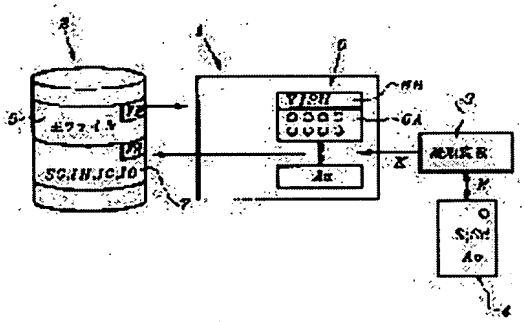
(21)Application number : 06-092992
(22)Date of filing : 06.04.1994

(71)Applicant : BULL CP 8
(72)Inventor : UGON MICHEL

(30)Priority
Priority number : 93 9304073 Priority date : 06.04.1993 Priority country : FR

(54) METHOD FOR SIGNING INFORMATION FILE AND DEVICE FOR IMPLEMENTING THIS METHOD

(57)Abstract:
PURPOSE: To shorten the calculation and verification time of a signature by taking at least a part of a file into consideration and generating a subfile and writing information, which can discriminate each part of a main file used for calculation of at least the signature, in this subfile and relating the subfile to the signature and signed files.
CONSTITUTION: A portable electronic object 4 is related to an information processor 1, and a calculation algorithm (ciphering) is expanded in the processor 1 and the object 4 so that a signature SG is a function of a secret key in the object and file contents. In this case, the processor 1 can expand a signature algorithm AS of at least a part of a main file EP stored in a part 5 of a large- capacity memory 2. Each time the signature is calculated, a subfile FS is generated which includes the signature SG and a parameter or information which discriminates data used for calculation of this signature, and it is registered in the subfile FS.



LEGAL STATUS

[Date of request for examination]	06.04.1994
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3050484
[Date of registration]	31.03.2000
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－13486

(43)公開日　平成７年(1995)１月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		8837－5L		
Ｇ０６Ｆ　12/00	５３７　Ｄ	8944－5B		

審査請求　有　　請求項の数25　ＦＤ　（全 14 頁）

(21)出願番号　特願平6－92992

(22)出願日　平成６年(1994)４月６日

(31)優先権主張番号　９３０４０７３

(32)優先日　1993年４月６日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　593023176
ブル・セー・ベー・８
フランス国、78430・ルーブシエンヌ、ベー・ベー・45、ルート・ドウ・ベルサイユ、68

(72)発明者　ミシエル・ユゴン
フランス国、78310・モルパ、リユ・デ・セパージユ、６

(74)代理人　弁理士　川口　義雄　（外２名）

(54)【発明の名称】　情報ファイルの署名方法及びそれを実施するための装置

(57)【要約】

【目的】　署名の計算及び検証時間の短縮可能な情報ファイルの署名方法及び装置を提供する。

【構成】　本発明は、メモリと処理回路を備え署名者の自由になる携帯式電子オブジェクト（４）の秘密メモリ・ゾーンに記憶された、署名者に固有であるがそれ自体は未知の、少なくとも１つの秘密データ（Ｓ；Ｓｄ）を考慮に入れて、情報処理装置（１、３、４）の回路に、ファイルの少なくとも１つの署名（ＳＧ）を計算させ、計算された署名を主ファイルに関連付けることからなる種類の、主情報ファイル（ＦＰ）の署名方法に関する。

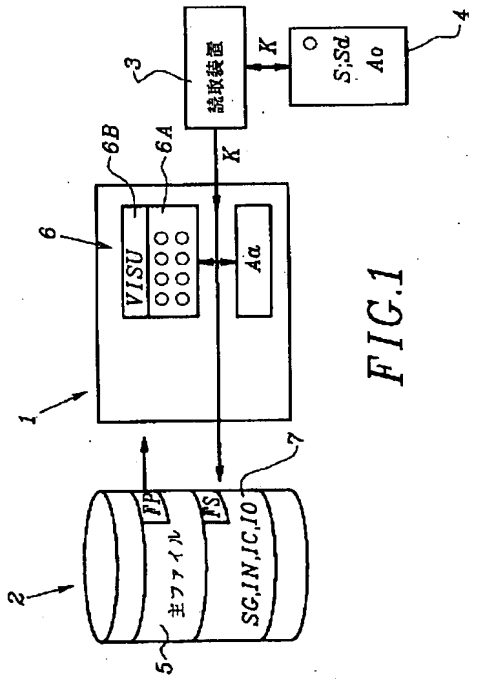


FIG.1

1

【特許請求の範囲】

【請求項１】　メモリと処理回路とを備え署名者が自由に使用できる携帯式電子オブジェクト（４）の秘密メモリ・ゾーンに記憶された署名者に固有の秘密データ（Ｓ；Ｓｄ）を少なくとも考慮に入れて、情報処理装置（１、３、４）の回路によってファイルの少なくとも１つの署名（ＳＧ）を計算させるステップと、計算された署名を主ファイルに関連付けるステップとからなるタイプの、主情報ファイル（ＦＳ）の署名方法であって、各署名の計算の際にさらに、署名が署名者の秘密データとファイルの考慮された各部分との関数となるように、主ファイルの少なくとも１つの部分を考慮に入れるステップと、この署名の計算に使われた主ファイルの各部分を識別するための情報（ＩＮ）を少なくともそこに書き込むステップと、副ファイルを対応する署名ならびに署名されたファイルに関連付けることからなるステップとを特徴とする情報ファイルの署名方法。

【請求項２】　副ファイルを対応する署名（ＳＧ）に関連付けるために、処理装置によって副ファイル内にこの対応する署名を書き込ませるステップからなることを特徴とする、請求項１に記載の方法。

【請求項３】　署名装置が、第１の計算アルゴリズム（Ａａ）を展開する処理装置（１）と、署名者の携帯式電子オブジェクト（４）とから構成され、補足情報（ＩＣ）、特に署名装置、すなわち署名の計算の際に実際に使われた装置（１）または第１アルゴリズム（Ａａ）あるいはその両方を識別するためのデータを副ファイルに書き込むステップからなることを特徴とする、請求項１に記載の方法。

【請求項４】　署名装置が、第１の計算アルゴリズム（Ａａ）を展開する処理装置（１）と、第２の計算アルゴリズム（Ａｏ）を展開する署名者の携帯式電子オブジェクト（４）とから構成され、携帯式オブジェクトの識別データ（ＩＯ）を副ファイルに書き込むステップからなることを特徴とする、請求項１に記載の方法。

【請求項５】　潜在的各署名者に固有の秘密データが、多様化されたデータ（Ｓｄ）、すなわち署名者ごとに異なるデータであることを特徴とする、請求項１に記載の方法。

【請求項６】　携帯式オブジェクトの識別データ（ＩＯ）が、署名の検証の際に、データを漏らさずに、署名検証装置の処理回路に、この署名の計算に使われたオブジェクトの秘密データ（Ｓｄ）を再計算させるためのデータを含むことを特徴とする、請求項１に記載の方法。

【請求項７】　携帯式オブジェクトの識別データ（ＩＯ）が、オブジェクトによって展開されたアルゴリズムを表す、言い換えれば利用されたオブジェクトのタイプを表すデータを含むことを特徴とする、請求項４に記載の方法。

【請求項８】　潜在的各署名者に固有の秘密データが、

2

非多様化データ（Ｓ）であることを特徴とする、請求項１に記載の方法。

【請求項９】　署名装置が、第１の計算アルゴリズム（Ａａ）を展開する回路を備えた処理装置（１）と、第２の計算アルゴリズム（Ａｏ）を展開する回路を備えた署名者の携帯式電子オブジェクト（４）とから構成され、署名者に固有の秘密データ（Ｓ；Ｓｄ）を、漏らさずに考慮に入れるために、外部データ（Ｅ）を作成し、それを処理装置の回路からオブジェクトの回路へ伝送するステップと、その後に第２アルゴリズム（Ａｏ）を展開し外部データ（Ｅ）と秘密データ（Ｓ；Ｓｄ）とを考慮に入れさせることによって、オブジェクトの回路にキー（Ｋ）を計算させるステップと、その後にこのキー（Ｋ）をオブジェクトの回路から処理装置の回路に伝送するステップと、最後に第１アルゴリズム（Ａａ）を展開し、キー（Ｋ）と少なくとも主ファイルの前記部分とを考慮に入れさせることによって、処理装置の処理回路に署名（ＳＧ）を計算させるステップとからなることを特徴とする、請求項１に記載の方法。

【請求項１０】　外部データ（Ｅ）が、処理装置（１）の処理回路によって自動的に、特にランダムに作成され、この外部データ（Ｅ）が、副ファイル（ＦＳ）の補足情報（ＩＣ）のうちに書き込まれることを特徴とする、請求項９に記載の方法。

【請求項１１】　外部データ（Ｅ）が、ファイルの署名の日付または時間あるいはその両方の関数であり、あるいはそれらから構成され、この外部データ（Ｅ）または署名の検証の際にそれを再計算するための情報あるいはその両方が、副ファイル（ＦＳ）の補足情報（ＩＣ）のうちに書き込まれることを特徴とする、請求項９に記載の方法。

【請求項１２】　外部データ（Ｅ）が、主ファイル（ＦＰ）から引き出された情報またはそれに関係する情報あるいはその両方から構成されることを特徴とする、請求項９に記載の方法。

【請求項１３】　外部データ（Ｅ）を構成する前記情報が、主ファイル（ＦＰ）からランダムに引き出され、この外部データを再構成するための情報が、副ファイル（ＦＳ）の補足情報（ＩＣ）のうちに書き込まれることを特徴とする、請求項１２に記載の方法。

【請求項１４】　署名装置が、処理装置（１）と、第２アルゴリズム（Ａｏ）を展開する回路を備えた署名者の携帯式電子オブジェクト（４）とからなり、署名者に固有の秘密情報（Ｓ；Ｓｄ）を漏らさずに考慮に入れるために、主ファイルの少なくとも前記部分を処理装置の回路からオブジェクトの回路へ伝送するステップと、その後第２アルゴリズム（Ａｏ）を展開し、前記部分と秘密データ（Ｓ；Ｓｄ）とを考慮に入れさせることによって、オブジェクトの回路に署名（ＳＧ）を計算させるステップと、その後にこうして計算された署名（ＳＧ）を

3

副ファイル（ＦＳ）に書き込むステップとからなることを特徴とする、請求項１に記載の方法。

【請求項１５】　署名の日付または時間あるいはその両方や主ファイルの名称またはヘッドあるいはその両方など署名の計算で考慮に入れるべき他の少なくとも１つのパラメータをオブジェクトの回路に伝送するステップと、こうして考慮された他の各パラメータを再発見するための情報を副ファイル（ＦＳ）に書き込むステップとからなることを特徴とする、請求項１４に記載の方法。

【請求項１６】　オブジェクト（Ａｏ）のアルゴリズムが、処理装置とオブジェクトと主ファイル（ＦＰ）及び副ファイル（ＦＳ）を含むメモリとの間でのパラメータ、データ、計算及び交換の全体を管理するように構成されることを特徴とする、請求項１４に記載の方法。

【請求項１７】　請求項１に記載の方法を実施することによって得られる、主情報ファイル（ＦＰ）に関連する決定された署名を検証するための方法であって、主ファイルに関連する副ファイルのおかげで、当該の署名を得るのに使われた主ファイルの各部分を識別するステップと、こうして識別された各部分を考慮に入れて、処理装置（１）の処理回路に署名（ＳＧ′）を再計算させるステップと、再計算された署名（ＳＧ′）を関連する署名（ＳＧ）と比較するステップと、再計算された署名を漏らさずに比較の結果を示すステップとからなることを特徴とする方法。

【請求項１８】　署名の計算に、主ファイルの前記部分以外のパラメータを考慮に入れる必要があり、計算の際に考慮に入れられた他の各パラメータを再発見または再計算するための補足データを識別するために、副ファイルを読み取るステップからなることを特徴とする、請求項１７に記載の方法。

【請求項１９】　主ファイルの内容を表示する手段（６Ｂ、１８）と、各署名者の自由になり、各署名者が、署名の計算の際に考慮に入れるために主ファイルの少なくとも一部分を選択できるようにする手段（６Ａ、１０、２０、２１）とを備えることを特徴とする、請求項１に記載の方法を実施するための装置。

【請求項２０】　ファイルの少なくとも一部分を選択するための手段（６Ａ、１０、２０、２１）が、ファイルの署名者によるファイルの１つまたは複数の部分の手動選択、あるいは処理装置（１）によるファイル全体の自動選択を可能にするように構成されることを特徴とする、請求項１９に記載の装置。

【請求項２１】　既にあるファイルに関連付けられている各署名の名称または順序を表示する手段と、１つまたは複数の署名をその検証のために選択する手段（１３、１４）と、計算中または検証中の署名の順序または名称を表示する手段とを備えることを特徴とする、請求項１９に記載の装置。

【請求項２２】　処理装置（１）が適当なアルゴリズム

4

を利用するように、計算中の署名に使われるまたは検証中の署名に使われた携帯式オブジェクト（４）の諸特性を処理装置（１）に指定する手段（“ＯＰＴＩＯＮＳ”）を備えることを特徴とする、請求項１９に記載の装置。

【請求項２３】　署名（ＳＧ）を検証するために、署名の計算の際に考慮された主ファイル（ＦＰ）の各部分以外の、署名の計算の際に考慮されたパラメータを、漏らさずに再発見または再計算できるように構成されたモジュールに結合された検証装置を備えることを特徴とする、請求項１９に記載の装置。

【請求項２４】　モジュールが、検証装置に接続できる、メモリとこのメモリの処理回路とを備えた携帯式電子オブジェクトであることを特徴とする、請求項２３に記載の装置。

【請求項２５】　署名者の自由になる、それらの署名者に固有の署名を計算するための、携帯式電子オブジェクトのうち少なくともいくつかが、これらのオブジェクトが、ファイルに署名するために、また非多様化秘密データ（Ｓ）と多様化秘密データ（Ｓｄ）のどちらを使って計算された署名を検証するためにも無差別に使用できるように、検証モジュールを形成するように構成されていることを特徴とする、請求項２４に記載の装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、情報ファイル（電子ファイルとも称す）の署名方法、署名の検証方法、及びこの方法を実施するための装置に関する。

【０００２】

【従来の技術】あらゆる性質の情報を情報処理手段を用いて様々な対話者間で交換することがますます増えてきている。たとえば、ファイルを２進情報の形で伝送する、電子メールの場合がそうである。

【０００３】ファイルに含まれる情報の性質または重要度に応じて、その発信者すなわち作成者を正しく識別することが必要なことがあり、あるいは資格のある人物がその同意を与えたまたはかかるファイルを有効であると確認したことを検証することが必要なこともあり、それも手書き文書やタイプ文書の場合よりもさらに確実な方法でそうする必要がある。実際に、タイプ文書の作成者やかかる文書に関与する資格のあるすべての人物は、文書に添えられた手書きの署名で識別することができる。

【０００４】文書の有効性確認の概念は、たとえばある種の行為の実行を認める目的で、１人または複数の人物が文書に署名または略署名しなければならない環境で生じる。公式文書、行政または会計印刷物、１人または複数の人物に権限を与えるあらゆる文書、あるいは複数の人物を巻き込むあらゆる文書（たとえば契約）の場合に特にそうである。

【０００５】ペーパ文書（手書きまたはタイプ）の場合

5

にはサポート・ペーパに署名が付けられるので、その作成者または有効性を確認した人物の識別を推測することが比較的容易であるが、電子ファイルではそうではない。実際に、電子ファイルは、論理値“０”または“１”をもつ一連のビットから構成される。その結果、かかるファイルに添付されたその作成者または有効性を確認した人物の識別の指示だけでは、所与の瞬間に存在するファイルが、前記の人物が署名または確認した時点にそれが存在した状態にあることを証明するには十分ではない。

【０００６】このため、各署名者ごとに処理回路に電子署名を計算させ、こうして計算された各署名をファイルと関連付けることにより、かかるファイルに電子的に署名を付けることが考案された。この電子署名は、ファイルの内容と１人の署名者または１つの署名者グループに固有の少なくとも１つのパラメータとの関数である。署名者の識別の検証手順は、処理回路に署名を再計算させ、この再計算された署名を関連する署名と比較することからなる。

【０００７】侵入者、すなわち署名する資格のない人物は、本来の署名者に固有のパラメータを手にしていないため、ファイルを修正しそれに整合性のある署名を関連付けることができない。同様に、複数の人物が文書に署名しなければならない環境では、少なくとも１人の人物が既に署名した後にファイルが修正されると、既に計算済みの各署名を整合性のある署名で置き換えることが不可能なことになる。

【０００８】このような署名の計算・検証方法は、フランス特許第２５１４５９３号明細書に記載されている。この特許は、米国特許第４６５６４７４号及び欧州特許第０７７２３８号に対応している。

【０００９】この方法は、潜在的各署名者に、マイクロコンピュータ・カード（チップ・カードとも称する）のような携帯式オブジェクトを与えることからなる。このカードのメモリに、そのオブジェクトの処理回路のみがアクセスできる秘密キーが格納されている。秘密キーは多様化されている。すなわち、オブジェクトごとに異なっており、異なる２つのオブジェクトが同じメッセージに同じ方式で署名できないようになっている。

【００１０】署名ステップは、厳密に言えば、オブジェクトを情報処理装置（その中でファイルが作成され、そこから他の装置にファイルが送られる装置でよい）に関連付け、署名が秘密キーとファイル内容との関数となるように装置中及びオブジェクト中で計算アルゴリズムを展開させることによってファイルに署名することからなる。

【００１１】秘密キーがオブジェクト外に漏れるのを避けるため、署名を完全にオブジェクト内部でその処理回路によって計算し、あるいはオブジェクトによって部分的結果を計算し、それを処理装置の回路に送ってそこで

6

計算を完了する。さらに、処理装置はたとえばデータ圧縮アルゴリズムを使用して計算を開始し、厳密にはオブジェクトが署名を計算する。署名は、その計算後にファイル及び署名者の識別に関係する情報と共に伝送される。

【００１２】検証ステップは、適当な装置の処理回路に、ファイルを漏らさずにその署名を再計算させ、次いでこの再計算された署名をファイルに付けられた署名と比較し、最後に比較の結果（この２つの署名が一致するか否か）だけを示すことからなる。再計算が可能になるのは、検証装置の処理回路が、ファイルと共に送られた署名者の識別に関する情報から署名者の多様化された秘密キーを漏らさずに再計算し、この再計算されたキーから署名を再計算することのできるアルゴリズムを含む。再計算されたキーは、その秘密の性質が保たれるように検証装置の回路の外部に漏らされない。再計算された署名が漏らされないのは、検証動作を観察していた侵入者が再計算の結果を私利のために利用できないようにするためである。

【００１３】

【発明が解決しようとする課題】しかしながら、これら既知の署名方法は、とりわけ、署名の計算と検証の際にファイル全体を考慮に入れる必要があるという不都合を示す。このため様々な理由から厄介なことが生じる可能性がある。

【００１４】第１の理由は、ファイルにただ１人の人物が署名しなければならない場合、あるいは誰もそれに修正を加えず複数の人物が署名しなければならない場合に該当するもので、ファイルが長すぎる場合に、署名の計算と検証のプロセスにかなりの時間がかかる可能性があることによる。これは、情報処理の目的と矛盾する。

【００１５】ところで、ファイル中には、敏感といえる情報とそうでない情報が存在する。敏感な情報とは、内容に関するものである。すなわち、合計ファイルの数値、報告書や手紙の特定の段落などである。敏感でない情報とは、形式に関するものである。たとえば、それがあると内容の変更なしにファイルの価値が高まり、それがなくてもまたは修正されても重要ではない、付随テキストなどである。

【００１６】第２の理由は、複数の人物が、ファイルのあるゾーンを修正するまたはファイルに情報を追加する権限を与えられて、ファイルに署名するよう仕向けられる場合に該当するもので、この場合、既知の方法では、最後の署名者の署名だけを真正であると宣言することができる。というのは、ファイルに対するそれぞれの修正または追加により、以前の署名を作成するのに使われたパラメータが修正されるからである。

【００１７】本発明の第１の目的は、従来の技術の方法に比べて署名の計算・検証時間を削減できるようにすることである。

7

【００１８】本発明の第２の目的は、同じファイルを場合によっては修正し、あるいは第１の署名者がその有効性を確認した後に追加を行って、複数の人物が署名できるようにすることである。

【００１９】

【課題を解決するための手段】上記の目的は、署名者の自由になる、メモリと処理回路とを備えた携帯式電子オブジェクトの秘密のメモリ・ゾーンに記憶された、署名者に固有のそれ自体は未知の少なくとも１つの秘密データを考慮に入れて、情報処理装置の回路にファイルの少なくとも１つの署名を計算させるステップと、計算された署名を主ファイルに関連付けるステップとからなる種類の主情報ファイルの署名方法であって、各署名の計算の際に、さらに、署名が署名者の秘密データとファイルの考慮される部分との関数となるように、ファイルの少なくとも一部分を考慮に入れるステップと、副ファイルを作成し、少なくともその署名の計算に使われた主ファイルの各部分の識別を可能にする情報をそこに書き込むステップと、副ファイルを対応する署名及び署名付きのファイルに関連付けるステップとからなることを特徴とする方法を提唱する本発明によって達成される。

【００２０】他の特徴によれば、副ファイルを対応する署名に関連付けるために、署名を副ファイルに書き込む。

【００２１】他の特徴によれば、各署名者の秘密データを、署名者の自由になるメモリと処理回路とを備えた携帯式電子オブジェクトの秘密のメモリ・ゾーンに記憶する。

【００２２】他の特徴によれば、好ましくは署名者に固有のデータを多様化して、異なる２人の署名者が同じファイルを同じ方式で署名できないようにする。この特徴により、たとえば前掲の特許明細書に記載の方法を実施することによって各署名者を再発見することにより、各署名者を識別することが可能になる。それにもかかわらず、多様化されていないデータ、すなわち少なくとも複数の署名者に共通するデータを利用することも、ファイルが権限のある人物によって署名されたことだけを知ればよく、それが誰かを厳密に知る必要はない場合には可能である。

【００２３】本発明による、計算されたファイルの決定された署名を検証する方法は、副ファイルのおかげで、最初の計算の際に使用されたものに対応する感知されたパラメータを考慮に入れた当該の署名を得るために使われた署名済みファイルの各部分を、処理回路に再計算させるために識別するステップと、再計算された署名を関連する署名と比較するステップと、比較の結果を示すステップとからなることを特徴とする。

【００２４】本発明は、従来技術の方法の安全性を保存しながら、より大きな柔軟さと多数の利点を持つので、特に有利である。

8

【００２５】具体的には、署名者がファイル全体に署名することを選択した時から、署名者はその内容全体が敏感な情報から構成されると推定するので、対応する署名に関連する副ファイルの情報は、この署名がファイル全体を用いて計算されたことを示すことになる。この場合、後の署名者がファイルを修正した場合、先の署名は整合しないものになる。一方、署名者は自分の順番が回ってきたとき全体的または部分的にそれに署名することもでき、あるいはそれに情報を追加し、その後で追加した情報の全部または一部に基づいて、あるいはこの追加を行う前にファイルが含まれていた情報の全部または一部に基づいて、自分の署名を計算することもできる。

【００２６】したがって、新規の各署名を計算すると、この新規の署名がその確立を可能にした情報と一緒に書き込まれた、新しい副ファイルが作成され、あるいはその副ファイル中に新しい登録が作成されることになる。

【００２７】この方法の他の利点は、ファイルにその作成者が署名した後にそのファイルの有効性を確認しなければならない人物が、ある部分の内容のみに対する同意を表明することが可能であることである。このため、有効性を確認しなければならない人物は、自分の署名の計算に、自分が同意するファイルの部分のみを考慮に入れさせることができる。

【００２８】本発明の他の諸特徴は、添付の図面を参照しながら以下の説明を読めば明らかになろう。

【００２９】

【実施例】図１に、本発明の好ましい実施例の装置の原理の概略図を示す。図のシステムは、署名の作成または検証に無差別に使用することができる。

【００３０】この装置は、情報ファイルを処理する能力を有するコンピュータなどの情報処理装置１を含む。装置１は、既知の形で、データまたはファイルを大量記憶する手段２を備える。記憶手段２は、磁気ディスケット、光ディスク、あるいは考えられるどんな記憶装置でもよい。

【００３１】さらに、好ましい実施態様では、装置１は、マイクロコンピュータ・カードなどの交換可能な携帯式電子オブジェクト（４）（交換可能電子サポートとも称する）の読取装置３に接続される。この電子オブジェクトは、既知のように、処理回路と秘密メモリ・ゾーンを含み、この秘密メモリ・ゾーンには、これらの処理回路からだけアクセス可能なデータが記録される。この秘密メモリ・ゾーンには各カード中で多様化された、すなわちカードごとに異なる、少なくとも１つの秘密データＳｄが含まれる。この秘密データにより、２つのカード内で展開され、２つのカードに適用される同じ入力データと各カード中で多様化されたデータとを考慮した同じ計算アルゴリズム（暗号化、署名など）が、カードごとに異なる結果を与える。したがって、この装置及び電子オブジェクトが、署名装置または検証装置を構成す

9

る。

【００３２】ある変形では、交換可能電子サポート４の秘密メモリ・ゾーンが多様化されたデータを含まず、特定のアプリケーション用のすべてのカードで同一の、あるいは特定のアプリケーション向けに、このアプリケーションに対して同一のアクセス権を有する人物に委ねられるすべてのカードで同一の秘密データＳのみを含む。実際に、この多様化は、すべてのまたは一部のユーザを互いに区別しなければならない場合に必要である。

【００３３】したがって、同じアプリケーションに関して、同じ階層レベルに属する、すなわち同一の署名能力またはアクセス権を有する、潜在的署名者間で秘密データを多様化することが可能である。一方、異なる階層レベル間には多様化が存在する。異なる階層レベルに属する複数の人物がファイルに署名するだけでよく、その識別を厳密に決定する必要のない、文書の検証だけが必要な環境では、この実施態様で十分である。

【００３４】また、潜在的署名者全体が、そのレベルには関係なく、同じ秘密データを持つことも可能である。この場合は、ファイルが権限を有する１人の人物によって署名されたことを単に検証することができる。

【００３５】もちろん、情報処理アプリケーションごとにデータを多様化する方が好ましい。

【００３６】装置１は、計算アルゴリズム、特にその大容量メモリ２の一部分５に格納される主ファイルＦＰの少なくとも一部分の署名アルゴリズムＡａを展開することのできる処理回路を含む。展開される瞬間に、アルゴリズムＡａはたとえば装置１の活動メモリの一ゾーンに登録される。

【００３７】さらに、装置１は、そのユーザとのインタフェース／対話手段６、特にキーボード６Ａ、スクリーン６Ｂを含む。マウスや音声認識装置など例示しなかった他の手段を含むこともできる。

【００３８】交換可能電子サポート４の役割は、読取装置３を介して装置１に、そのメモリに格納された多様化秘密データＳｄまたは非多様化秘密データＳの関数であるキーＫを提供することである。このキーＫの作成方法は後で説明する。

【００３９】キーＫは、署名アルゴリズムＡａの展開時に、署名ＳＧがこのキーＫと主ファイルＰの少なくとも一部分との関数となるようにするために、装置１の処理回路によって考慮される。

【００４０】後で説明するが、署名の計算で考慮される主ファイルの部分の選択は、署名者が行うことも、システムによって自動的に行うこともできる。

【００４１】本発明によれば、署名ＳＧの検証を可能にするために、各署名を計算するたびに、この署名ＳＧと、その計算に使われたデータを識別するためのパラメータまたは情報とを含む、新しい副ファイルＦＳが作成され、または副ファイルへの新規の登録が行われる。この副ファイルＦＳは装置１によって作成され、次いでその大容量メモリ２の部分７に書き込まれる。

10

【００４２】具体的には、副ファイルＦＳは、その構成パラメータのうちに、署名の計算に使われた主ファイルＦＰの部分を再発見するための情報ＩＮを含んでいる。それはこれらの部分のメモリ・アドレスに関係する情報のことも、主ファイル内で上記部分を再発見するためのすべての情報のこともある。

【００４３】署名の計算に使われる主ファイルＦＰの部分を再発見するためのこれらの情報ＩＮに加えて、副ファイルＦＳは補足情報ＩＣを含むことができる。

【００４４】まず、署名計算アルゴリズムＡａは、装置ごとに異なることが考えられる。同じ装置を署名の計算または検証に無差別に使用できなければならないことを想起されたい。ところで、所与の瞬間に、たとえばソフトウェアの進化により、署名を行わなければならない場合に、署名の計算に使われた装置が、検証に使われた装置よりもソフトウェアのより古いバージョンを利用することがあり得る。さらに、この進化とは無関係に、この２つの装置が全く異なるソフトウェアを計算に利用することもあり得る。また、署名者が複数の場合に、同一のファイルの署名が、異なるソフトウェアを利用する違った装置で計算されたことがあり得る。言い換えれば、異なる装置を署名の計算に使用することができる。

【００４５】そのため、この場合、副ファイルＦＳを含む補足情報ＩＣのうちで、装置を識別するためのデータ、すなわち署名の計算時に実際に利用された装置またはアルゴリズムあるいはその両方が見つかる。

【００４６】先に指摘したように、キーＫは携帯式電子オブジェクト４によりそれに含まれる多様化秘密データＳｄまたは非多様化秘密データＳから計算される。多様化秘密データＳｄを含む電子オブジェクトは、署名者を明確に識別しなければならなくなるごとに使用しなければならない。一方、署名者がある限られたグループに属する権限を有する人物であることを検証するだけでよい場合は、秘密データが多様化されている必要はない。それがこのグループのすべての人物に共通したものであるだけで十分である。これらの原理は、従来の署名方法で知られている。

【００４７】キーＫの計算は、電子オブジェクト内でその処理回路に記憶されたアルゴリズムＡｏを展開させるステップと、このアルゴリズムによってそのメモリに含まれる多様化秘密データＳｄまたは非多様化秘密データＳと、装置内で作成され装置から電子オブジェクトに送られる外部データＥとを、キーＫが同時に秘密データＳｄまたはＳと外部データＥとの関数となるように考慮に入れさせるステップとからなる。

【００４８】電子オブジェクトの秘密データが多様化されている場合、検証のために利用される装置が、後でキーＫを再計算する目的で、その秘密データを漏らすこと

11

なく再発見できることが必要である。

【００４９】これは、たとえば、本明細書の冒頭に記載し、参照によりその教示を本明細書に合体する、どちらかの特許明細書に開示された方法を適合させて実施することにより、それを漏らさずかつ署名に使用された電子オブジェクトを自由に使わせずに、ある電子オブジェクトの多様化秘密データを再計算させることのできる既知のあらゆる方法を実施することにより、行うことができる。

【００５０】どちらか一方の特許明細書に開示された、本発明の適合された方法は、副ファイルＦＳにそれを書き込むことにより、たとえば補足情報のうちで、検証装置の固有の回路により多様化されたデータを漏らさずに再計算または再発見させることのできる電子オブジェクトの識別データＩＯを、本ファイルＦＰ及び署名ＳＧに関連付けることからなる。これらの識別データは、たとえば、サポートの秘密メモリ・ゾーンに登録されているｑ個の基本キーのうちのｐ個の基本キーのアドレスを表すｐ個のパラメータから構成することができ、多様化秘密データはこれらｐ個のアドレスに含まれる情報の組合せによって構成される。

【００５１】さらに、先に言及した通り、電子オブジェクトはアルゴリズムＡｏを展開する。一般にこのアルゴリズムは、ＲＯＭまたはＰＲＯＭ型の不揮発性メモリに移植され、電子オブジェクトのタイプごとに異なる可能性がある。そのため、電子オブジェクトの識別データＩＯはその電子オブジェクトによって展開されたアルゴリズムを、言い換えれば利用される電子オブジェクトのタイプをも表すことができる。

【００５２】この場合、後で詳しく説明する署名の検証の際に、特定の制御モジュールが検証装置に関連付けられる。このモジュールの構造については、後で署名検証の諸ステップの説明に関して詳しく説明する。

【００５３】外部データＥの作成は署名の瞬間に様々な方式で実施され、署名装置の処理回路に登録されたアルゴリズムＡａに依存する。

【００５４】ある実施態様では、この外部データＥは、装置１の処理回路によって自動的に作成される。これはたとえばランダム・データでよい。その場合は、装置１は乱数発生機構を含む。

【００５５】このような自動作成の場合、この外部データＥは、検証装置がキーＫを再発見できるように、副ファイルＦＳの補足情報ＩＣのうちにも書き込まれる。

【００５６】ある実施態様では、外部データＥはファイルの署名の日時の関数であり、あるいはそれから構成される。この場合、外部データＥ自体、または署名検証の瞬間に再検査を可能にする情報、すなわち日時に相関された情報が、副ファイルＦＣの補足情報ＩＣのうちに書き込まれる。

【００５７】別の実施態様では、外部データＥは、主ファイルＦＰ自体から抽出されたまたは主ファイルに関係する情報から構成される。これらの情報の記憶位置及び性質は予め知ることができ、あるいは装置の処理回路により署名の計算の瞬間にランダムに決定することができる。

12

【００５８】したがって、一変形では、外部データＥは、ファイルのすべての第１（８ビット）バイトからまたは署名の計算で考慮されるファイルの第１部分のすべての第１バイトから選ばれた、所定の数ｎ個のバイトから構成される。

【００５９】この数ｎは、利用するバイトの記憶位置と同様に、最終的に固定することができる。この場合、外部データＥは、検証装置によるアルゴリズムＡａの決定から、この外部データＥがどのように作成されたかが推論できるので、副ファイル中で参照することはとてもできない。

【００６０】別の変形では、外部データＥは、ファイルの名称あるいはファイルのヘッダまたはサイズ、一般にはそのファイルから引き出されるすべての情報と相関される。

【００６１】別の変形では、利用されるバイトの数ｎまたは記憶位置が、外部データの作成の瞬間に装置によってランダムに決定される。この場合、外部データＥまたはこの外部データを再計算するための情報、たとえば利用されるバイトの数または記憶位置が、副ファイルＦＳの補足情報ＩＣのうちに書き込まれる。

【００６２】まとめると、外部データＥが作成されたとき、キーＫが署名者の携帯式サポート３中でこの外部データＥとこのサポートに含まれる秘密データＳまたはＳｄとの関数として計算される。

【００６３】－　場合に応じて、外部データＥあるいは検証装置に再発見させるための情報が、副ファイルＦＳに書き込まれる。

【００６４】－　サポートの秘密データが多様化データＳＤである場合、検証装置に再発見させるための識別情報ＩＯがサポートから署名装置へ送られ、署名装置によって副ファイルＦＳに書き込まれる。

【００６５】－　署名ＳＧが、キーＫとファイルの少なくとも一部とから計算され、次いで副ファイルに書き込まれる。

【００６６】－　ファイルのどの部分が署名の計算に使われたかを決定するための情報が、副ファイルに書き込まれる。

【００６７】もちろん、複数の署名者が関与する場合は、各署名者ごとに異なる副ファイルまたは登録が作成される。その結果、複数の副ファイルを同一の主ファイルに関連付けることが可能となり、あるいは副ファイルが登録も当該の署名も有することになる。

【００６８】１つまたは複数の署名の検証は、どちらか一方または両方の署名者によって、あるいはこの検証用

13

に構成された装置を自由に使用できるとの条件で第三者によって行うことができる。実際に、この装置は、各署名の計算に使われた装置と類似していなければならない。さらに、この計算に使われた装置自体であってもよい。

【００６９】検証操作は、署名の確立に使われたのと同じパラメータを使って各署名を再計算するステップと、再計算された署名を副ファイルに書き込まれた対応する署名と比較するステップとからなる。そのために、検証装置は処理回路と比較回路を備えている。

【００７０】検証を観察していた侵入者が結果を私利のために利用するのを避けるため、検証装置は、再計算された署名が処理回路及び記憶回路の外に決して漏れず、比較の結果だけが指示されるように構成された、処理回路と記憶回路を有することが好ましい。したがって、再計算に必要なデータは、検証装置のメモリの秘密ゾーン中で処理され、再計算された署名は、比較の結果が示された後に抹消される。

【００７１】署名を再計算されたできるようにするため、先に指摘した通り、検証装置はまずその署名を得るために使われたキーＫを再計算できなければならない。ところで、このキーは署名者に固有の携帯式電子オブジェクトのメモリの秘密ゾーンに格納されている多様化秘密データＳｄまたは非多様化秘密データＳから計算されたことを想起されたい。

【００７２】秘密データが多様化されたものである場合、先に言及したように前掲の特許明細書に記載されている方法を適合させることにより、装置は、メモリの秘密ゾーンと、このゾーンに含まれる情報の処理回路とを備える特定の制御モジュールを含むことができ、これらの情報がこのモジュールから出るのを避けるようになっている。

【００７３】ある実施態様では、このモジュールは装置中に常駐する。

【００７４】一変形では、このモジュールは、署名者が利用したものと類似のメモリとマイクロコンピュータを備えた携帯式電子オブジェクト４によって構成される。

【００７５】好ましい実施例では、署名者が自由に使用できる携帯式電子オブジェクトのいくつかまたはそれぞれが、署名の検証モジュールとして利用できる。

【００７６】したがって、電子オブジェクトは署名を可能にするだけでなく、同じファミリーのカードによって、すなわち、たとえばベースの同じ秘密データから出発してあるいは前掲の特許明細書に記載されているようにして作成された多様化秘密データＳｄを有するカードによって計算されたすべての署名の検証も可能にする。

【００７７】この場合、どの電子オブジェクトの多様化データも、署名を検証する目的で、同じファミリの電子オブジェクトのいくつかまたはそれぞれによって再計算または再構成することができる。もちろんこの場合、検

14

証に使われる電子オブジェクトは再計算可能な署名も再構成された多様化データも供給しない。

【００７８】これにより、同一の電子オブジェクトを誰が使って署名し検証することもできるが、署名者が他人の署名を複製することができないようになる。

【００７９】したがって、前掲の特許明細書の教示を適用する場合、制御モジュールの秘密ゾーンが可能なｑ個のパラメータを含むだけで十分であり、副ファイル内で、ある署名ＳＧに関連する識別情報ＩＯを読み取ると、この識別情報によって指定されるアドレスの内容を決して漏らさずに読み取ることにより、モジュールがその処理回路中でこの署名の計算に使われた電子オブジェクトの秘密データＳｄを再構成することが可能になる。

【００８０】データが多様化されたものでない場合は、装置が、秘密データＳがその中で再生されるメモリの秘密ゾーンを有するモジュールと、この秘密ゾーンのデータがこれらの処理回路によってしかアクセス可能でないように構成された処理回路とに結合されていれば十分である。ある実施例では、このモジュールが装置に常駐し、処理回路が装置の処理回路であってよい。一変形では、モジュールが携帯式電子オブジェクトから構成される。好ましい実施例では、署名者が自由にできる各携帯式電子オブジェクトを検証モジュールとして利用できる。

【００８１】検証装置は、この目的で署名段階で副ファイルＦＳに書き込まれた情報（外部データＥ自体、日時など）のおかげで、外部データＥを再発見できるように構成されている。

【００８２】次に、外部データＥと、このモジュールのおかげで再発見され、したがって署名の計算時に利用されていたものに対応することが感知された、多様化秘密データまたは非多様化秘密データとからキーＫが、再計算される。このキーＫの再計算では、秘密データが漏らされず、したがってこの秘密ゾーンに関連する回路によって、すなわち実施態様に応じて装置の回路または携帯式電子オブジェクトの回路によって実施されることが必ず必要である。

【００８３】装置の処理回路は次に、副ファイルＦＳから、主ファイルのどの部分が元の署名の計算に使われたかを決定し、再計算されたキーＫと主ファイルの前記部分とを考慮に入れて署名ＳＧ′を秘密裏に再計算する。

【００８４】最後に、比較回路が、再計算された署名ＳＧ′を副ファイル中で読み取られた署名ＳＧと比較し、次いで装置は、自らが備える表示手段を用いて検証を行う人物に比較の結果だけを示す。

【００８５】したがって、前記の好ましい実施例は、オブジェクト中でキーＫを計算させ、次いで装置の処理回路にこのキーＫと主ファイルＦＰの少なくとも１つの部分との関数として署名を計算させる。

【００８６】一変形では、署名はオブジェクト中で計算

15

され、したがって外部データＥを生成する必要がない。この場合、装置に記録されたアルゴリズムＡａは、その処理回路がファイルの選択された部分と、場合によっては日時や名称、サイズなど考慮に入れるべき他の複数のパラメータとを生成し、オブジェクトに送るようになっており、オブジェクトの回路が計算終了時にファイルの諸部分と情報処理装置から受け取った他のパラメータとの関数である署名ＳＧを復元し、次いでこの署名を副ファイルＦＳに書き込むために装置に送る。したがって、匹敵するがキーを情報処理装置に転送する必要のない結果が得られる。一方、他の１つまたは複数のパラメータが考慮に入れられる場合は、それを再発見するための情報を副ファイルに書き込まなければならない。

【００８７】オブジェクトによって署名を計算するこの場合、装置の回路が基本的機能を有するように設計される。情報処理装置に記憶されるアルゴリズムＡａは、オブジェクト及び大容量メモリに含まれるファイルとの交換が可能なように最小限に減らされる。

【００８８】しかし、この変形では、好ましい態様よりも進んだ計算の可能性とアルゴリズムを有する、携帯式電子オブジェクトの使用が必要である。実際に、前記の好ましい態様では、オブジェクトの処理回路が入ってくるオーダに応答して、それに含まれる秘密データＳまたはＳｄと外部データとの関数である結果を供給することが予めできるだけでよい。

【００８９】本発明の物理的及び論理的実現は当業者の技量の範囲に含まれるものであり、詳しく説明する必要はない。

【００９０】主ファイルＦＰの署名は、主ファイルとその副ファイルＦＳが、計算に使われたのと同じ装置上にあるとき、あるいは主ファイルとその副ファイルＦＳが異なる装置に転送された後に、検証することができる。

【００９１】この転送は、本発明の目的ではない。これは既知のどんな手段や方法によっても実施できる。データ行ごとの電子転送でも、ディスケットなどの物理的サポートを用いた転送でも、他のどんなタイプのデータ転送でもよい。明らかに、主ファイルとそれに関連する副ファイルを、この操作をそこで実施したい場合、署名の検証を実施できる装置、すなわち適切な論理構造を有する装置に転送することが望ましい。

【００９２】本発明を容易に実施するには、署名者または署名の検証者であるシステム・ユーザとの容易な対話、すなわち人間工学的で気持ちのよい対話が可能なシステムを実現することが好ましい。

【００９３】したがって、本発明を、ＭＩＣＲＯＳＯＦＴ社の“ＷＩＮＤＯＷＳ”環境の下で機能するような対話ウィンドウの利用が可能な、ファイル処理ツール上で実施することが好ましい。

【００９４】図２に、あるファイルに付随する署名の計算または検証を開始するためにオープンすることのできる基本的対話ウィンドウを示す。

16

【００９５】アプリケーションのタイトル８が、ウィンドウ上部のタイトル・バー９に現れており、メニュー・バー１０でメニューが利用可能である。

【００９６】最初のメニュー“ＭＯＤＥ”（モード）で、「署名」モードまたは「署名検証」モードを選択することができる。

【００９７】第２のメニュー“ＦＩＣＨＩＥＲ”（ファイル）で、装置のメモリに含まれ、ユーザが署名したいまたは署名を検証したいファイルのタイプを何でも選択することができる。たとえば、テキスト・ファイル、データ・ファイル、図面ファイルなどである。

【００９８】第３のメニュー“ＳＥＬＥＣＴＩＯＮ”（選択）には、少なくとも「署名」モードが活動状態のときにアクセスできる。これを使うと、後で詳しく述べる「手動選択」機能または「自動選択」機能にアクセスすることができる。

【００９９】第４のメニューの“ＯＰＴＩＯＮＳ”（オプション）で、たとえばある署名に既に使われたサポートを選択し、あるいは新しいサポートの諸特性を決めることができる。これらの概念については後で詳しく説明する。

【０１００】最後に、エイド・メニュー“？”が存在することもある。

【０１０１】図３及び４は、メニュー“ＦＩＣＨＩＥＲ”によってあるファイルが活動化され、メニュー“ＭＯＤＥ”によって署名検証モードが活動化されたときにオープンできるウィンドウの２つの変形を示す。これらの変形には、最小の違いしかないが、それについては必要になるたびに明らかにする。

【０１０２】検証モードが活動化されているとき、メニュー“ＳＥＬＥＣＴＩＯＮ”がアクセス可能である必要のないことが好ましい。一方、メニュー“ＦＩＣＨＩＥＲ”と“ＭＯＤＥ”はアクセス可能でなければならない。

【０１０３】最初の画面“ＳＯＵＲＣＥ”（ソース）１１が現れる。これは有効性を確認されたファイルの状態に関する情報を含み、その名称と、署名されているか否かと、サイズとファイルの日付けと、それが配列されているリストとを示す。

【０１０４】さらに、第２の画面“ＳＩＧＮＡＴＵＲＥ”（署名）１２は、このファイルに関連する署名の番号または名称あるいはその両方を示す。

【０１０５】図３の変形では、この第２画面１２の各署名が、第１ゾーン１３に示された名前、この場合は“Ｐｉｅｒｒｅ”、“Ｐａｕｌ”などによってマークされる。図４の変形では、この第２画面１２の各署名が、装置によってデフォルトとして与えられ、第１ゾーン１３に示される順序番号“Ｓｉｇｎ　１”、“Ｓｉｇｎ　２”によってマークされる。

17

【０１０６】第２ゾーン１４は、活動状態の署名が、その名前（図３）または番号（図４）によって示される。

【０１０７】図３の第３の画面“ＩＮＦＯＲＭＡＴＩＯＮ”（情報）１５では、検証中の署名“Pierre”がファイル全体に基づいて計算されたことを示す“selection totale”（全体選択）の語が表示されている。図４に対応する画面では、検証中の署名“Ｓｉｇｎ　１”がファイルの一部分に基づいて計算されたことを示す“selection manuelle”（手動選択）の語が表示されている。

【０１０８】その上、この第３画面１５のゾーン１６には、検証中の署名の計算に使われたサポートの名称が示されている。

【０１０９】“ＯＫ”または“ＳＴＯＰ”ボタンは、この画面１５に置かれ、たとえばマウスまたはキー６Ａでポインタが移動されたためにアクセス可能となり、検証の開始または中止を可能にする。

【０１１０】画面１５の別のゾーン１７には、“ＯＫ”ボタンによって検証開始が有効とされた後の検証計算の進行状況が百分率で表示される。さらに、ゾーン１７は、その長さで進行状況を示すバーを表示することができる。

【０１１１】署名の作成または追加中に開くことのできるウィンドウを図５及び６に示す。「署名」モードの選択は、“ＭＯＤＥ”メニューから行われ、“ＭＯＤＥ”メニューには、アプリケーションの開始時に、または「検証」モードから、あるいはもちろん「署名」モード自体が有効とされた時にアクセス可能となる。

【０１１２】「署名」モードが活動化された時に、デフォルトによりファイルの全体選択が行われる。すなわち署名がファイル全体から計算されることが好ましい、しかし、後述するように、ファイルの１つまたは複数の部分の手動選択も実施できる。

【０１１３】「署名」モードが活動化されると、メニュー全体がアクセス可能になる。

【０１１４】図５に、「署名」モードと手動選択が活動化されている時に開くウィンドウを示す。

【０１１５】開かれたウィンドウは、情報画面１５に活動状態のモードが署名計算モードであることが示され、“selection manuelle”の語が平文で表示されている点以外は、図３及び４のそれに類似している。

【０１１６】デフォルトによって選択が行われる場合、図には示していないが、図５のそれとただ１つの違いがあるウィンドウが開かれることに留意されたい。すなわち、情報の画面１５に、“selection manuelle”の代りに“selection totale”の語が表示されている。

【０１１７】その上、署名中のファイルに関する名称と情報が第１画面“ＳＯＵＲＣＥ”に表示され、進行中の署名の名称と番号が第２画面１２の第２ゾーン１４に表示される。

【０１１８】最後に、第３画面１５の特定のゾーン１６に、進行中の署名の計算に使われるサポートの名称が書き込まれる。

18

【０１１９】好ましい一実施例では、情報画面１５の“ＯＫ”ボタンを操作すると、任意にまたはデフォルトによって全体選択が選ばれたとき、署名計算が開始される。

【０１２０】一方、この好ましい実施例では、手動選択を選ぶと、図６に表すウィンドウが開かれる。このウィンドウは、マウスまたは処理装置のキー６Ａのタッチによって移動されるカーソルなど、それ自体は既知のカーソルによって、ファイルの内容を表示し、いくつかのゾーンを選択することができる。

【０１２１】以前のウィンドウに表示されていた画面“ＳＯＵＲＣＥ”と“ＳＩＧＮＡＴＵＲＥ”が、唯一の画面１８で置き換えられ、画面１５“ＩＮＦＯＭＡＴＩＯＮ”が存在し続けるとき、画面１８にファイルの内容が表示される。

【０１２２】ファイルの１つまたは複数の部分の選択は、マウスまたはキー・タッチによってカーソルを移動することにより、手動で行うことができる。この図６の例は、３７バイトから構成されるテキスト・ファイルのある部分１９（ブロックとも称する）の選択を示している。情報画面は、ブロック数と選択されたバイトの総数を示す。

【０１２３】このウィンドウは、ファイルの異なる部分を調べる可能性を与える目的でファイルを画面に対して移動するための、それ自体は既知の１つまたは複数の直線状セレクタ２０、２１を備えることができる。第１のセレクタ２０は、たとえば現行ページ内での移動を可能にし、第２のセレクタ２１はページ間の移動を可能にする。

【０１２４】最後に、“ＯＫ”ボタンを操作すると、選択が有効になり署名の計算が開始する。

【０１２５】“ＯＰＴＩＯＮＳ”メニューは、たとえば署名の際に新規サポートの諸特性をシステムに指定し、あるいは検証の際に既に指定されていたサポートの諸特性を調べることができる。

【０１２６】したがって、署名にどのタイプのカードを使うかをシステムに指定したい新規署名者がその有効性を確認しなければならない。

【０１２７】カードなどその特性が他人によって既に再入力されているサポートを新規署名者が使用する場合、このメニューによってそれを指定する。

【０１２８】有効性確認により、図７のウィンドウに一致するウィンドウ“ＣＡＲＴＥ”（カード）が開かれる。このウィンドウは、新規署名の計算に使われる新規サポートの定義の様々なパラメータを捕捉するための諸ケースを含んでいる。異なるアルゴリズムまたは様々に多様化されたキーを含むサポートが計算時に識別でき、最終的検証が行えるのは、このメニューのおかげであ

19

る。

【０１２９】したがって、とりわけこのメニューのおかげで、当該のサポートでアクセスが可能になるアプリケーション“Ref Appli”（テキスト、テーブルなどの処理）を示すことができる。さらに、システムが正しく機能できるように、関係するサポートのタイプとそれに含まれるキーのバージョン（“Ref cle”、“versioncle”）を正確に識別することができる。さらに一般的に、このメニューは、計算及び検証のためにサポートが自由に使用できるように、あるサポートに関する必要なすべてのパラメータをシステムに指定することができる。

【図面の簡単な説明】

【図１】本発明を実施するための好ましいシステムの原理を示す概略図である。

【図２】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

【図３】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

20

【図４】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

【図５】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

【図６】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

【図７】署名段階または検証段階でのユーザとシステムの対話のある画面の好ましい配置を示す図である。

【符号の説明】

1　情報処理装置
2　大容量メモリ
3　読取装置
4　交換可能電子サポート（携帯式電子オブジェクト）
5　主ファイル（ＦＰ）
6　インタフェース／対話手段
7　副ファイル（ＦＳ）

【図１】

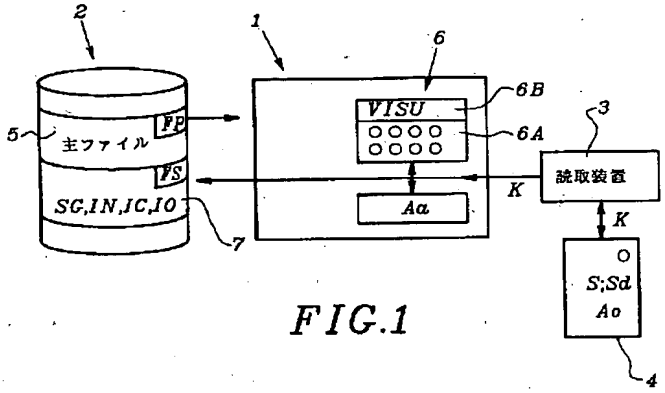


FIG.1

【図２】

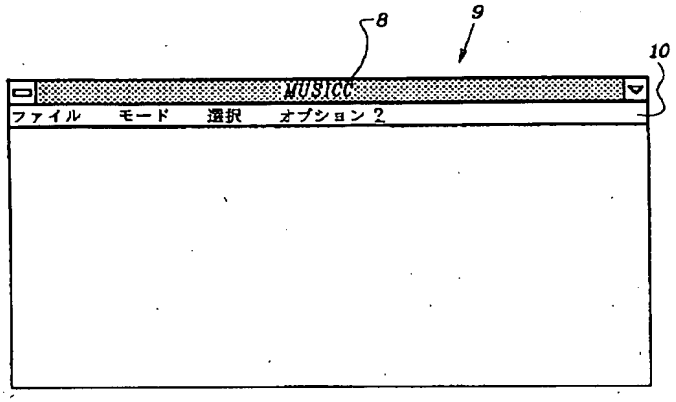


FIG.2

【図３】

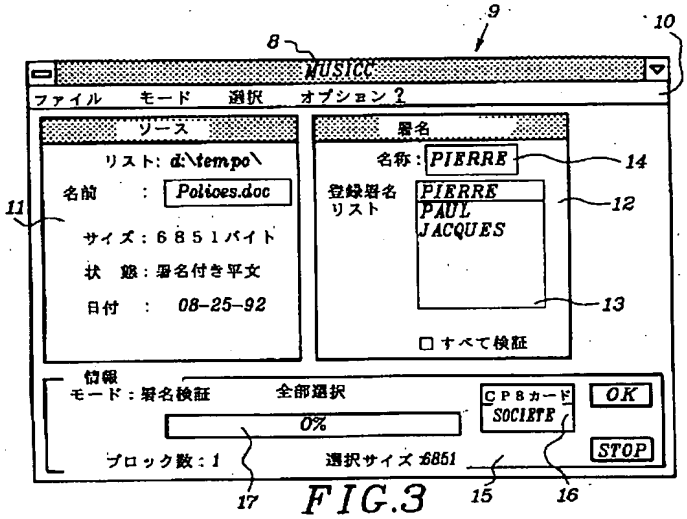


FIG.3

【図４】

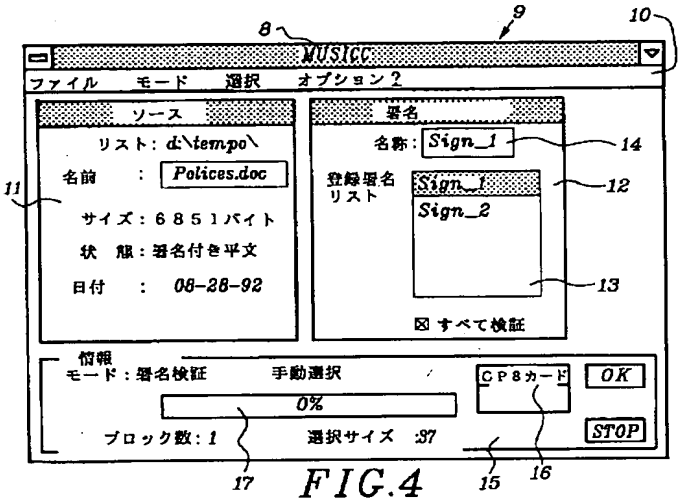


FIG.4

【図５】

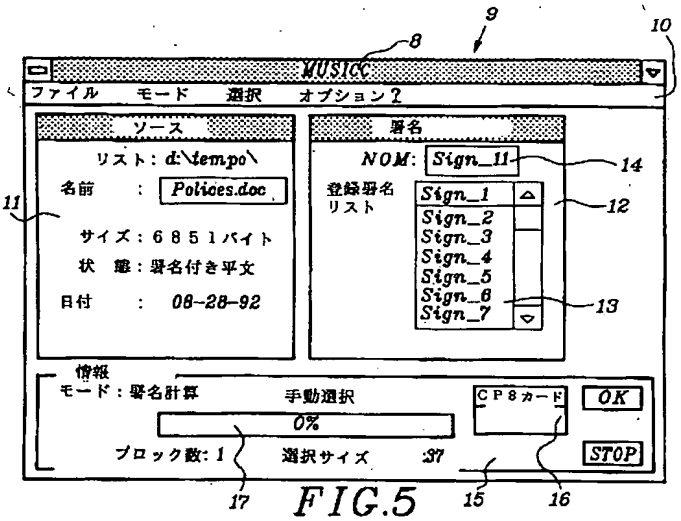


FIG.5

【図６】

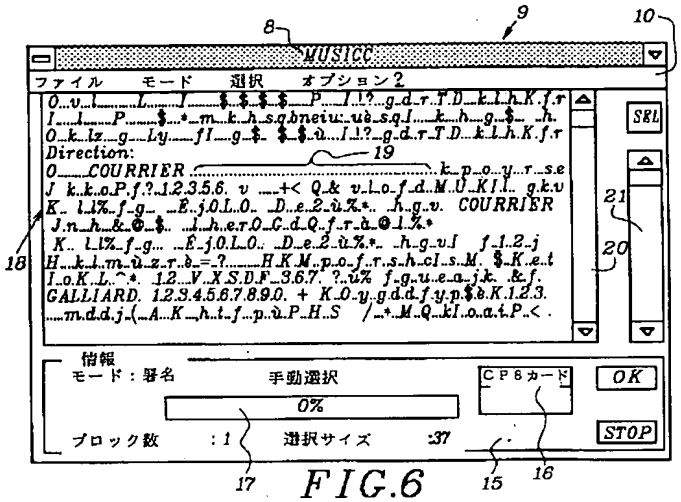


FIG.6

【図７】

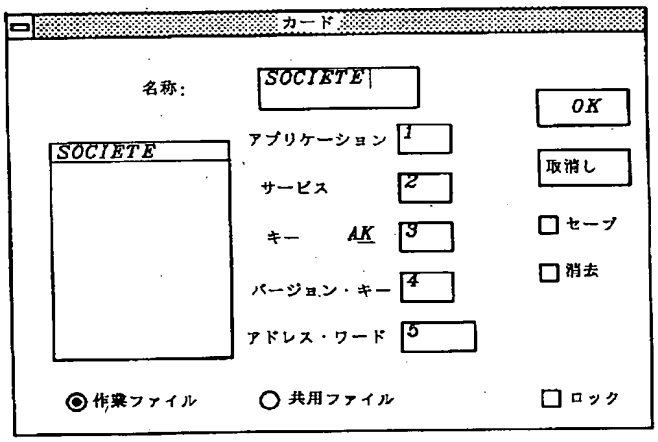


FIG.7